AMENDMENTS TO THE CLAIMS

No amendments are made by this Response. The below listing of claims is provided for the Examiner's convenience.

<u>Listing of Claims:</u>

1.   (Original) A method comprising:

    receiving content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;

    receiving a base key corresponding to an M of N level of access, where L<=M<=N; and

    deriving lower level keys based on the base key, the lower level keys being used to access content having an M level of access or lower.

2.   (Original) The method of claim 1, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level

key and a one-way hash function of an adjacent higher level key.

3. (Original) The method of claim 1, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.

4. (Original) A method comprising:

receiving a request for content at an M level of access, the content comprising a set of attributes having L through N levels of access, where L<N, and each level of access being represented by a grid point on a grid, and corresponding content being decryptable by a key corresponding to the level of access;

transmitting a base key corresponding to the M level of access; and

transmitting a D-dimensional matrix for each attribute in the set of attributes, where D corresponds to a number of attributes of the content, and where the matrix comprises matrix values for determining how to generate a lower level key for decrypting content represented by a given grid point on the grid.

5. (Original) The method of claim 4, wherein a given lower level key in a 2 dimensional matrix, where X comprises a first matrix, and Y comprises a second matrix, is generated by at least one of:

the equation $K_{i,j} = X_{i,j} \wedge H(K_{i+1,j})$; and

the equation $K_{i,j} = Y_{i,j} \wedge H(K_{i,j+1})$,

where $X_{i,j}$ and $Y_{i,j}$ each comprises a matrix value corresponding to content attributes at a level of access represented by a grid point (i, j), and $H(K_{i+1,j})$ and $H(K_{i,j+1})$ each comprise a one-way hash value of a higher level key.

6. (Original) The method of claim 4, wherein a given lower level key in a 1 dimensional matrix represented by X is generated by the equation $K_i = H(K_{i+1})$.

7. (Original) A method comprising:

creating a hierarchy of keys, where each key is used to encrypt content having a set of attributes, and having one or more levels of access, and each key corresponds to a level of access; and

applying each of the keys to the content to create a plurality of sections of encrypted content, each section being a portion of the content, and each successive section of the content improving the set of attributes of the content.

8. (Original) The method of claim 7, additionally comprising creating a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content.

9.   (Original) The method of claim 7, wherein the hierarchy of keys are related

       by a cryptographic strength one-way function.

10.   (Original) The method of claim 7, wherein an attribute comprises

       resolution.

11.   (Original) A machine-readable medium having stored thereon data

       representing sequences of instructions, the sequences of instructions

       which, when executed by a processor, cause the processor to perform the

       following:

       receive content comprising a set of attributes having L through N levels of

              access, where L<N, and content at a given level of access being

              decryptable by a corresponding key;

       receive a base key corresponding to an M of N level of access, where

              L<=M<=N; and

       derive lower level keys based on the base key, the lower level keys being

              used to access content having an M level of access of lower.

12.   (Original) The method of claim 11, additionally comprising instructions that

       cause the processor to receive a D-dimensional matrix for each attribute in

       the set of attributes, wherein D corresponds to a number of attributes of

       the content, and wherein the matrix comprises matrix values for

       determining how to generate a key corresponding to a given section of the

       content, and the instructions cause the processor to derive lower level

       keys based on the base key comprises, for a given lower level key, using

Docket No.: 42390P11149   6   Utility Patent Application
Application No.: 09/896,537

a function based on a matrix value corresponding to the lower level key and a one-way function of an adjacent higher level key.

13. (Original) The method of claim 11, wherein the instructions cause the processor to derive lower level keys based on the base key comprises, for a given lower level key, by using a modular exponentiation of a higher level key.

14. (Original) An apparatus comprising:

at least one processor; and

a machine-readable medium having instructions encoded thereon, which when executed by the processor, are capable of directing the processor to:

receive content comprising a set of attributes having L through N levels of access, where L<N, and content at a given level of access being decryptable by a corresponding key;

receive a base key corresponding to an M of N level of access, where L<=M<=N; and

derive lower level keys based on the base key, the lower level keys being used to access content having an M level of access of lower.

15. (Original) The method of claim 14, additionally comprising instructions that

cause the processor to receive a D-dimensional matrix for each attribute in

the set of attributes, wherein D corresponds to a number of attributes of

the content, and wherein the matrix comprises matrix values for

determining how to generate a key corresponding to a given section of the

content, and the instructions cause the processor to derive lower level

keys based on the base key comprises, for a given lower level key, using

a function based on a matrix value corresponding to the lower level key

and a one-way hash function of an adjacent higher level key.

16. (Original) The method of claim 14, wherein the instructions cause the

processor to derive lower level keys based on the base key comprises, for

a given lower level key, by using a modular exponentiation of a higher

level key.

17. (Original) An apparatus comprising:

means to receive content comprising a set of attributes having L through N

levels of access, where L<N, and content at a given level of access

being decryptable by a corresponding key;

means to receive a base key corresponding to an M of N level of access,

where L<=M<=N; and

means to derive lower level keys based on the base key, the lower level

keys being used to access content having an M level of access of

lower.

Docket No.: 42390P11149   8   Utility Patent Application
Application No.: 09/896,537

18.   (Original) The method of claim 17, additionally comprising means to

      receive a D-dimensional matrix for each attribute in the set of attributes,

      wherein D corresponds to a number of attributes of the content, and

      wherein the matrix comprises matrix values for determining how to

      generate a key corresponding to a given section of the content, and the

      means to derive lower level keys based on the base key comprises, for a

      given lower level key, using a function based on a matrix value

      corresponding to the lower level key and a one-way hash function of an

      adjacent higher level key.

19.   (Original) The method of claim 17, wherein the means to derive lower level

      keys based on the base key comprises, for a given lower level key, using

      a modular exponentiation of a higher level key.

20.   (Original) A method comprising:

      receiving encrypted content comprising a set of attributes having L

            through N levels of access, where L<N, and each level being

            accessible by a corresponding key;

      receiving a base key corresponding to an M of N level of access, where

            L<=M<=N;

      deriving lower level keys based on the base key, the lower level keys

            being used to access content having an M level of access or lower;

            and

using a given lower level key to decrypt the content at a corresponding

level.

21. (Original) The method of claim 20, additionally comprising receiving a D-dimensional matrix for each attribute in the set of attributes, wherein D corresponds to a number of attributes of the content, and wherein the matrix comprises matrix values for determining how to generate a key corresponding to a given section of the content, and said deriving lower level keys based on the base key comprises, for a given lower level key, using a function based on a matrix value corresponding to the lower level key and a one-way function of an adjacent higher level key.

22. (Original) The method of claim 20, wherein said deriving lower level keys based on the base key comprises, for a given lower level key, using a modular exponentiation of a higher level key.